Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2016)

Ports and Impact Analysis Testing

1. **Introduction.** This document provides requirements for determining minimal ports and services for cyber assets subject to the North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards.

2. **Ports and Services.** The requirements for enabling only those ports and services that are necessary for normal and emergency operations are addressed in CIP 005-R2.2 for access points into the Electronic Security Perimeter (ESP) and in CIP 007-R2 for all cyber assets subject to the NERC CIP Reliability Standards. Compliance with the above referenced requirements also includes documenting the rationale and justification for enabling or disabling ports and services, as well as, identifying any compensating measures applied to mitigate the risk exposure where the unnecessary ports and services cannot be disabled due to technical limitations of the configuration capability of the cyber asset.

   A. **Step 1: Determining Baseline Configurations.** While a minimal set of ports and services are required for an operating system, additional ports and services may be necessary to support the function of the server, workstation, or personal computer. Hosted applications such as iFIX and database applications such as Oracle will require additional ports and services in addition to those that support the operating system alone. Vendor documentation and Security Technical Implementation Guides provide information to initially identify minimum ports and services. However, functional testing will be necessary to ensure that the operating system and hosted applications function properly after disabling all unnecessary ports and services. Internet Protocol (IP) enabled industrial assets such as Programmable Logic Controllers (PLCs) and protection relays identified as critical cyber assets (CCA) require testing and interaction with the vendor to determine the baseline configuration. While these devices require specific ports and services for operations, they typically include a broad set of capabilities for configuration. It is not uncommon for these devices to have telnet, HTTP, and SNMP ports open for remote access. In these situations, operational decisions are necessary to determine which ports and services will be primary or needed for emergency access, and which ones must be disabled.

   B. **Step 2: Documenting the Baseline.** Once all testing and research activities associated with Step 1 are completed, the authorized ports and services must be documented. System administrators must document and maintain the system ports and services baseline. The documentation must also identify known vulnerabilities for services with a high potential for security control failure that could not be disabled. This activity will support the mapping of compensating measures to be identified in Step 3. An inventory for each CCA must be maintained that clearly lists:

(1) the necessary ports and services,

(2) ports and services that have been enabled (where this may vary from necessary ports and services), and

(3) if applicable, those ports and services that cannot be disabled due to technical limitations.

C. **Step 3: Implementing and Identifying Compensating Measures.** CIP 007-R2.3 requires that in cases where unused ports and services cannot be disabled due to the technical limitations, compensating measures applied to mitigate the risk of exposure must be documented accordingly. An example of a compensating measure for ports that cannot be disabled includes the use of firewalls and routers at the access points to restrict communication to those ports from outside the ESP boundary. An electronic monitoring capability for detecting unnecessary network traffic is also recommended as a compensating measure. The documentation shall include the mapping of all unnecessary ports and services, services with known high risk vulnerabilities and exploits, and the related compensating measures implemented to mitigate the risk of exposure. The documentation produced may be utilized in the creation of a Technical Feasibility Exception associated with ports and services that cannot be disabled for a particular asset.

3. **Test Procedures.** CIP 007-R1 requires the development and execution of "test procedures" to ensure that "significant changes" to cyber assets subject to the NERC CIP Reliability Standards do not adversely affect existing cyber security controls. A "significant change," as defined in the NERC CIP Reliability Standards, includes the installation or update of: security patches; cumulative service packs; vendor releases; and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

A. **Step 1: Test Procedure Development and Documentation.** The test procedure must be designed to ensure that the cyber security controls have not been negatively impacted. For example, cyber security controls may include: accounts (password and account lockout settings); auditing (events, privilege use, logon, etc.); user rights (permissions or restrictions for the user or groups of users); security options (file or object permissions, system configurations such as encryption, interactive logon, banner displays); ports; and services.

(1) **Determine Existing Security Controls.** Not all cyber assets support the security controls identified above. Accordingly, an initial effort of test procedure development is required to determine which security controls exist for a particular

cyber asset and document how each control is employed for a particular device. A warning banner displayed as part of a start-up “script” or as a security configuration “setting” is considered a security control. Operator console security settings enforced by a local policy or via a group policy “pushed” to the cyber asset from a domain controller is considered a security control. Account permissions enforced by a database application or via the local operating system is also a security control. In every case, the developed test procedure shall identify the applicable cyber security control and validate the cyber asset’s specific implementation of the control.

(2) **Test Procedure Execution.** The test procedure must be executed in a manner that minimizes any potential adverse affect upon an operational system. One method of addressing this issue is to include an initial section of the documentation as an “assumption or constraint.” Information in this section must address the approved and recommended context for executing the procedure such as: restricted to a test environment, restricted on off-peak hour of operations, or approved for testing during normal operations. If approved for testing during operations, all actions necessary to minimize any potential negative affect must be documented and clearly stated as mandatory, optional, or recommended.

B. **Step 2: Text Execution and Documentation.** Documentation of all testing and test results related to significant changes must be maintained for each cyber asset subject to the NERC CIP Reliability Standards. The testing documentation shall include:

(1) date and time of test,

(2) a description of how the test environment reflects the production environment (test network, etc.),

(3) test justification (type of significant change, i.e. security patch, vendor upgrade),

(4) name of individual or individuals executing the test,

(5) test results (to include failure or success), and

(6) any revisions to the test procedure resulting from a failed test.